



**You have downloaded a document from
RE-BUŚ
repository of the University of Silesia in Katowice**

Title: O bazie fundamentalnej ciała cyklotomicznego

Author: Joanna Wuwer

Citation style: Wuwer Joanna. (1972). O bazie fundamentalnej ciała cyklotomicznego. "Prace Naukowe Uniwersytetu Śląskiego w Katowicach. Prace Matematyczne" (Nr 2 (1972), s. 95-96)



Uznanie autorstwa - Użycie niekomercyjne - Bez utworów zależnych Polska - Licencja ta zezwala na rozpowszechnianie, przedstawianie i wykonywanie utworu jedynie w celach niekomercyjnych oraz pod warunkiem zachowania go w oryginalnej postaci (nie tworzenia utworów zależnych).



UNIwersYTET ŚLĄSKI
W KATOWICACH



Biblioteka
Uniwersytetu Śląskiego



Ministerstwo Nauki
i Szkolnictwa Wyższego

JOANNA WUWER

O bazie fundamentalnej ciała cyklotomicznego

W książce Z. I. BOREWICZA i I. R. SZAFAREWICZA ([1], str. 129) sformułowany jest w charakterze problemu do udowodnienia następujący lemat, który często bywa pomocny przy wyznaczaniu bazy fundamentalnej ciała.

LEMAT. *Jeśli Θ jest pierwiastkiem wielomianu Eisensteina $f(x) = x_n + a_1x^{n-1} + \dots + a_n$ względem liczby pierwszej p (a_i — całkowite, $p \mid a_i$, $i = 1, \dots, n$, $p^2 \nmid a_n$), to p nie dzieli indeksu $(O:M)$ ordynku¹⁾ $M = \langle 1, \Theta, \dots, \Theta^{n-1} \rangle$ w ordynku maksymalnym O ciała $Q(\Theta)$.*

W oparciu o ten lemat, w sposób szczególnie prosty, można udowodnić na przykład twierdzenie o bazie fundamentalnej ciała cyklotomicznego $Q(\zeta)$, gdzie $\zeta^{p^n} = 1$.

TWIERDZENIE. *Niech ζ będzie pierwiastkiem pierwotnym stopnia p^n z jedności, p -liczba pierwsza, $n \geq 1$. Wtedy baza potęgowa $1, \zeta, \dots, \zeta^{\varphi(p^n)-1}$ jest bazą fundamentalną ciała $Q(\zeta)$ (φ — funkcja Eulera).*

D o w ó d. Wielomianem minimalnym liczby ζ jest

$$\begin{aligned} f(x) &= \frac{x^{p^n} - 1}{x^{p^{n-1}} - 1} = x^{p^{n-1}(p-1)} + x^{p^{n-1}(p-2)} + \dots + x^{p^{n-1}} + 1 = \\ &= \prod_{0 < i < p^n, (i, p) = 1} (x - \zeta^i) \end{aligned}$$

stopnia $s = \varphi(p^n)$. Zbiór $1, \zeta, \dots, \zeta^{s-1}$ jest bazą ciała $Q(\zeta)$.

Weźmy pod uwagę Z -moduły $M = \langle 1, \zeta, \dots, \zeta^{s-1} \rangle$ i $M' = \langle 1, \lambda, \dots, \lambda^{s-1} \rangle$, gdzie $\lambda = 1 - \zeta$. Z równości $\lambda = 1 - \zeta$ wynika, że $M' \subset M$ i podobnie z $\zeta = 1 - \lambda$ wynika, że $M \subset M'$, a więc moduły M i M' są równe. Niech O oznacza ordynek maksymalny ciała $Q(\zeta)$. Ponieważ ζ jest liczbą algebra-

¹⁾ Termin „ordynek”, zaproponowany przez prof. A. SCHINZLA, jest polskim odpowiednikiem angielskiego „order”, niemieckiego „Ordnung” i rosyjskiego „порядок”.

iczną całkowitą, więc $M' = M \subset O$. Stąd dla wyróżników $D(M')$ i $D(O)$ ordynków M' i O zachodzi $D(M') = (O : M')^2 D(O)$. Lecz $D(M') = D(M)$ jest potęgą liczby pierwszej p ([3], str. 71), skąd wynika, że $(O : M')$ jest także potęgą liczby p o wykładniku ≥ 0 . Z drugiej strony, zauważmy, że λ jest pierwiastkiem wielomianu EISENSTEINA $f(1 - x)$ względem liczby p ([2], str. 90, zad. 669), więc na mocy lematu $p \nmid (O : M')$. Zatem $(O : M') = 1$ tzn. $O = M' = M$.

PRACE CYTOWANE

- [1] З. И. Борович и И. Р. Шафаревич: *Теория чисел*, Москва, 1964.
- [2] Д. К. Фаддеев и И. С. Соминский: *Сборник задач по высшей алгебре*, Москва, 1964.
- [3] H. MANN: *Introduction to Algebraic Number Theory*, Columbus, 1955.

JOANNA WUWER

ON THE INTEGRAL BASIS OF A CYCLOTOMIC FIELD

Summary

Using a lemma formulated below the author gives a simple proof that $1, \zeta, \dots, \zeta^{s-1}$, $s = \varphi(p^n)$, is an integral basis of the field $\mathbb{Q}(\zeta)$, where ζ is a primitive root of unity of degree p^n .

LEMMA. *If Θ is a root of an Eisenstein polynomial with respect to the prime number p , then p does not divide the index $(O : M)$ of the order $M = \langle 1, \Theta, \dots, \Theta^{n-1} \rangle$ in the maximal order O of the field $\mathbb{Q}(\Theta)$.*

This lemma appears as a problem in [1], p. 129.

Oddano do Redakcji 2. 4. 1970 r.